警告：切勿侵犯版權

閣下將瀏覽的文章/內容/資料的版權持有者為消費者委員會。除作個人非商業用途外， 閣下不得以任何形式傳送、轉載、複製或使用該文章/內容/資料，如有侵犯版權，消費者委員會必定嚴加追究法律責任，索償一切損失及法律費用。

《消費者委員會條例》第二十條第(1)款其中有規定，任何人未經委員會以書面同意，不得發布或安排發布任何廣告，以明示或默示的方式提述委員會、委員會的刊物、委員會或委員會委任他人進行的測試或調查的結果，藉以宣傳或貶損任何貨品、服務或不動產，或推廣任何人的形象。有關該條文的詳情，請參閱該條例。

本會試驗的產品樣本由本會指定的購物員，以一般消費者身份在市面上購買，根據實驗室試驗結果作分析評論及撰寫報告，有需要時加上特別安排試用者的意見和專業人士的評論。對某牌子產品的評論，除特別註明外，乃指經試驗的樣本，而並非指該牌子所有同型號或不同型號的產品，也非泛指該牌子的所有其他產品。

本會的產品比較試驗，並不測試該類產品的每一牌子或同牌子每一型號的產品。

本會的測試計劃由本會的研究及試驗小組委員會決定，歡迎消費者提供意見，但恕不能應外界要求為其產品作特別的測試，或刊登其他非經本會測試的產品資料。

網上投資從保密開始

網上投資戶口向來「不認人」，任何人只要通過身份認證——目前主要是輸入自設的帳戶登入名稱及密碼，就可以登入及使用戶口。根據證券及期貨事務監察委員會的數字，在截至2017年3月31日止的18個月期間，有12間持牌法團舉報了27宗網絡保安事件，當中大部分為黑客入侵網上投資戶口。要保護自己的投資，首要保護自己的戶口登入資料。

防範社交工程圈套

黑客要入侵和操控用戶的網上投資戶口，先要取得認證用戶身份的密碼，除了利用電腦病毒入侵電腦和手機之外，他們也可以使出各種社交工程詭計。

社交工程屬於仿冒詐騙的伎倆，網絡釣魚是其中一種常見的招數，做法一般是大量散播附有病毒連結的偽冒電郵、網頁、社交網頁短訊及手機應用程式，要求用戶輸入個人資料。不慎中計，就有可能洩露重要的個人資料。

此外，騙徒也可以偽裝成朋友和親屬，或者是一些大家信任和熟悉的機構人員，例如銀行職員或警察，透過電話或電郵聯絡用戶，哄騙用戶提供個人資料。

黑客入侵戶口後如何圖利？

黑客用盜來的戶口買賣股票，是為了炒高散貨。首先，他們會僱用不同人士開立戶口，囤積一些流通量低、容易炒作的細價股，然後用盜來的戶口買入該等細價股。待該等細價股股價炒上後，黑客就大舉拋售自身持股套利。由於進行第三方戶口轉帳需要雙重認證，所以被盜戶口的資金一直未有離開戶口，然而有關細價股股價變動，卻為戶口帶來重大的帳面損失。

保密要訣

針對黑客攻擊，我們必須謹記以下安全守則：

- **視戶口登入資料為高度機密，任何情況下都不要向其他人透露：**騙徒可以冒認任何人包括你的中介人向你索取資料，如收到不明來歷的電郵，或見到不尋常的彈出畫面或視窗，要求你提供個人資料及密碼，切勿上當，如有懷疑，可向中介人求證，但切勿使用可疑電郵所提供的聯絡方法。
- **避免在社交網頁張貼敏感資料：**現時人們常用社交網頁與朋友溝通，在分享個人資訊時，要小心謹慎，不要張貼與登入戶口或重設戶口密碼有關的資料，例如出生日期、寵物名稱等，以防黑客看到。
- **密碼是保護網上投資戶口的重要防線：**我們不應貪圖方便或易記，使用容易破解的密碼。「123456」、「qwerty」、「111111」、「987654321」、「password」和「1q2w3e4r」等與鍵盤排列相關的密碼，都是一些高危但偏偏卻是最常見的密碼。而從字典裏找字詞，或用自己的個人資料作密碼，亦並不安全。反之，我們要設定一些與個人資料無關的密碼，最好至少有8個以上的字母，而視乎長度要求，你亦可以把密碼設定成詞組，或用記憶術來設定密碼，令密碼難以破解，例如「I have 2 dogs and 1 cat」可以寫作「Ih2d&1c」。謹記定期轉換密碼，不要重複使用同一密碼。
- **採用雙重認證：**要減低戶口被盜用的風險，可能需要加入密碼認證以外的身份認證，作雙重認證。用戶在輸入自設的帳戶登入名稱和密碼作第一步認證後，需要進行第二步認證，較普遍的是輸入由手機短訊發出或保安編碼器產生的一次性密碼，亦有採用數碼證書或生物認證。現時，當我們使用網上銀行服務轉帳至未經登記的第三者戶口時，就要進行雙重認證。
- 不要使用公共場所的電腦登入網上投資戶口。
- 當我們進行網上交易時，不要同時進行其他網上活動或連接其他網址，完成交易後，記得備存或打印交易紀錄或確認通知，供日後查核。
- 日常奉行良好的上網習慣，包括定期用最新的防毒軟件來偵察和掃除任何惡意軟件。

資料來源：錢家有道（由投資者教育中心管理，並獲教育局及四家金融監管當局支持）